NexDAST

NeuraLegion

Новое поколение инструментов динамического тестирования безопасности приложений

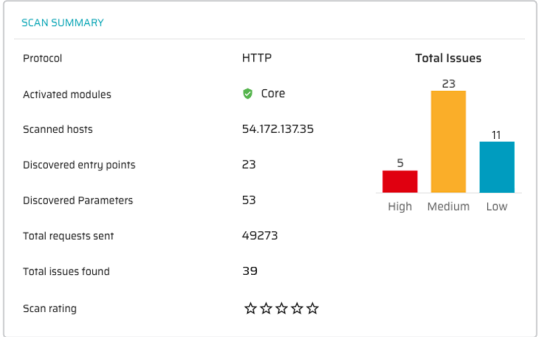
Автоматизированное и масштабируемое тестирование безопасности в темпе DevOps

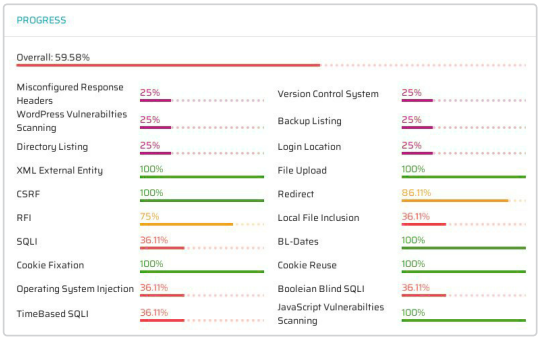
Общие сведения

NexDAST — это отмеченное наградами решение для тестирования безопасности приложений, web, предоставляемое по модели SaaS. Оно автоматически сканирует и выявляет уязвимости в приложениях, веб-сервисах, интерфейсах WebSocket и API.

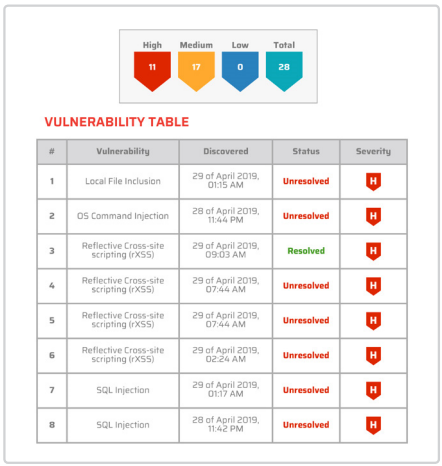
В отличие от других решений класса DAST, которые способны выявлять только уязвимости из обновляемых вручную списков, NexDAST также использует высокоэффективную базу знаний собственной разработки, в которой содержатся сведения обо всех уязвимостях нулевого дня, обнаруженных с помощью технологии AIAST® компании NeuraLegion.

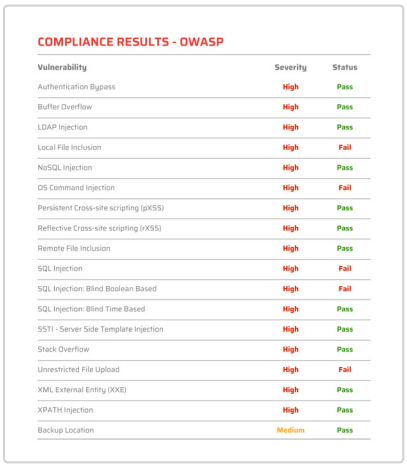
Решение NexDAST не генерирует ложных срабатываний, является масштабируемым и отлично подходит для применения в компаниях любого размера. Оно обеспечивает полную интеграцию и автоматизацию тестирования веб-приложений, гарантируя мгновенную экономию операционных и капитальных расходов за счет ускоренного цикла DevOps.





Высочайшие стандарты нормативного соответствия





- **Полная автоматизация и масштабируемость при поиске уязвимостей в веб-приложениях**
- **Простая интеграция с инструментами разработки и тестирования**
- **Создание отчетов в реальном времени, включая OWASP Top 10, PCI DSS и другие**
- **Обнаружение и устранение в темпе DevOps**

- **Поставляется по модели SaaS**
- **Поддержка стандартов OWASP Top 10 и др.**
- **Интеграция с инструментами SDLC, CD/CI**
- **Мгновенные отчеты**
- **Полное отсутствие ложных срабатываний**
- **Рекомендации по исправлению**

FORTIS
+7(495)260-0113
fortis.ru/Neuralegion
neuralegion@fortis.ru

NexDAST

NeuraLegion

Новое поколение инструментов динамического тестирования безопасности приложений

Основные возможности

Удобство использования

По умолчанию NextDAST — облачное решение, не требующее затратной интеграции и сложной настройки. Просто войдите в систему и запустите сканирование либо воспользуйтесь API-интерфейсом. Также возможно развертывание в частном облаке или на площадке заказчика.

Отсутствие ложных срабатываний

Решение NexDAST не генерирует ложных срабатываний и сообщает только о реальных подтвержденных уязвимостях, избавляя от необходимости проверять и фильтровать все отчеты. Это дает возможность быстрее устранять проблемы и сдавать продукт в эксплуатацию.

Мгновенные отчеты

Результаты сканирования доступны в реальном времени на панели управления или в виде загружаемых отчетов. Они включают в себя рекомендации по устранению обнаруженных уязвимостей и улучшению кибербезопасности.

Комплексное, тщательное тестирование

Продукт выявляет технические уязвимости из списка OWASP Top 10 и все уязвимости нулевого дня, которые были обнаружены технологией AIAST® и занесены в нашу уникальную базу знаний. Он обеспечивает самое тщательное сканирование среди всех решений класса DAST, представленных в данный момент на рынке.

Управление нормативным соответствием

При тестировании безопасности приложений поддерживаются стандарты ISO27001, PCI DSS, HIPAA, NIST 800 Series и другие отраслевые нормативы.

Интеграция с инструментами SDLC, CD/CI

Наше масштабируемое решение может быть полностью интегрировано в жизненный цикл разработки ПО, обеспечивая тестирование безопасности в темпе, который задает DevOps. Интеграция возможна через технологических партнеров или открытые API.

Интеграция безопасности в цикл разработки

GitHub slack circleci Jenkins JIRA

Раннее выявление, быстрое устранение

Чем раньше в процессе разработки ПО выявляются уязвимости, тем выше безопасность и дешевле исправление. NexDAST дает всем вовлеченным в процесс разработки — как новичкам, так и профессионалам — возможность быстро обнаруживать и устранять критические уязвимости в приложениях, находящихся в среде разработки, тестирования или эксплуатации.

Благодаря NexDAST вы можете тестировать больше приложений и делать это быстрее, а отсутствие ложных срабатываний помогает сосредоточиться на устранении выявленных дефектов. Процедуры тестирования безопасности оказываются полностью интегрированными в процесс разработки ПО.

ОТЗЫВ КЛИЕНТА EXCELLENCE Investments

«NexDAST обнаружил уязвимости, которые остались незамеченными при сканировании другими инструментами и, что еще важнее, при ручном тестировании. Его интеграция в конвейер SDLC обеспечила полную автоматизацию, повысила качество DevSecOps и мгновенно начала окупаться».

Геннадий Гринберг, директор по ИБ

FORTIS

+7(495)260-0113

fortis.ru/Neuralegion

neuralegion@fortis.ru